CAIS-Alerta: Resumo dos Boletins de Segurança Microsoft - Agosto/2014

Microsoft Security Bulletin Summary for August 2014

[RNP, 14.08.2014-, revisão 01]

A Microsoft publicou nove (9) boletins de segurança em 12 de agosto de 2014 que abordam ao todo 37 vulnerabilidades em produtos da empresa. A exploração dessas vulnerabilidades permite a execução remota de código, elevação de privilégio e desvio de recurso de segurança.

Até o momento da publicação desse alerta, não foram divulgados códigos de exploração para as vulnerabilidades listadas.

Severidade

- **Crítica**
    - **MS14-051 - Atualização de segurança cumulativa para o Internet Explorer**
    - **MS14-043 - Vulnerabilidade no Windows Media Center pode permitir a execução remota de código**
- **Importante**
    - **MS14-048 - Vulnerabilidade no OneNote pode permitir a execução remota de código**
    - **MS14-044 - Vulnerabilidades no SQL Server pode permitir a elevação de privilégio**
    - **MS14-045 - Vulnerabilidades nos drivers de modo kernel podem permitir a elevação de privilégio**
    - **MS14-049 - Vulnerabilidade no serviço Windows Installer pode permitir a elevação de privilégio**
    - **MS14-050 - Vulnerabilidade no Microsoft SharePoint Server pode permitir a elevação de privilégio**
    - **MS14-046 - Vulnerabilidade no .NET Framework pode permitir o desvio de recurso de segurança**
    - **MS14-047 - Vulnerabilidade no LRPC pode permitir o desvio de recurso de segurança**
- **Moderada**
- **Nenhum boletim**
- **Baixa**

- **Nenhum boletim**

O sistema de classificação de severidade das vulnerabilidades adotado pelo CAIS nesse resumo é o da própria Microsoft. O CAIS recomenda que se aplique, minimamente, as correções para vulnerabilidades classificadas como crítica e importante. No caso de correções para vulnerabilidades classificadas como moderadas, o CAIS recomenda que ao menos as recomendações de mitigação sejam seguidas.

- **Crítica** Vulnerabilidades cuja exploração possa permitir a propagação de um worm sem a necessidade de interação com o usuário.
- **Importante** Vulnerabilidades cuja exploração pode resultar no comprometimento de confidencialidade, integridade ou disponibilidade de dados de usuários ou a integridade ou disponibilidade de recursos de processamento.
- **Moderada** Exploração é mitigada significativamente por fatores como configuração padrão, auditoria ou dificuldade de exploração.
- **Baixa** Uma vulnerabilidade cuja exploração seja extremamente difícil ou cujo impacto seja mínimo.

Correções disponíveis

Recomenda-se atualizar os sistemas para as versões disponíveis em:

- Microsoft Update
- Windows Server Update Services

Mais informações

- Resumo do Boletim de Segurança da Microsoft de agosto de 2014
- Microsoft TechCenter de Segurança
- Microsoft Security Response Center - MSRC
- Microsoft Security Research & Defense - MSRD
- Central de Proteção e Segurança Microsoft

Identificador CVE (http://cve.mitre.org):
CVE-2014-4060, CVE-2014-1820, CVE-2014-4061, CVE-2014-0318, CVE-2014-1819,
CVE-2014-4064, CVE-2014-4062, CVE-2014-0316, CVE-2014-2815, CVE-2014-1814,
CVE-2014-2816, CVE-2014-2774, CVE-2014-2784, CVE-2014-2796, CVE-2014-2808,
CVE-2014-2810, CVE-2014-2811, CVE-2014-2817, CVE-2014-2818, CVE-2014-2819,
CVE-2014-2820, CVE-2014-2821, CVE-2014-2822, CVE-2014-2823, CVE-2014-2824,

CVE-2014-2825, CVE-2014-2826, CVE-2014-2827, CVE-2014-4050, CVE-2014-4051,
CVE-2014-4052, CVE-2014-4055, CVE-2014-4056, CVE-2014-4057, CVE-2014-4058,
CVE-2014-4063, CVE-2014-4067

O CAIS recomenda que os administradores mantenham seus sistemas e aplicativos sempre atualizados, de acordo com as últimas versões e correções oferecidas pelos fabricantes.

Os Alertas do CAIS também são oferecidos no formato RSS/RDF e no Twitter:
http://www.rnp.br/cais/alertas/rss.xml
Siga @caisrnp.